

BSI veröffentlicht Richtlinie zum sicheren E-Mail-Transport

Mit der Richtlinie "BSI TR-03108 Sicherer E-Mail-Transport" will das Bundesamt für Sicherheit in der Informationstechnik (BSI) die E-Mail-Anbieter dazu bringen, endlich flächendeckend die vorhandenen und nutzbaren Sicherheitsstandards einzusetzen.



Das BSI will die E-Mail-Anbieter dazu bringen, flächendeckend vorhandene Sicherheitsstandards einzusetzen.

Foto: wavebreakmedia - shutterstock.com

Rund neun Monate wurde an der Richtlinie mit Fachleuten in den Räumen des Bonner Innenministeriums gearbeitet. Vertreter von Open-Xchange haben ebenso mitgewirkt wie unser Partner Heinlein Support. Das Ergebnis kann sich meiner Meinung nach sehen lassen.

Die Richtlinie fordert nichts, was Provider nicht bereits heute erfüllen können. Sie enthält nichts revolutionär Neues, aber eben auch keinen faulen Kompromiss in der Sache. Die Messlatte liegt angemessen hoch: Technisch genau auf dem Stand der Zeit. Fakt ist dennoch, dass einige

Anbieter die Anforderungen der Richtlinie noch nicht erfüllen und sich entsprechend strecken müssen - und dies ist durchaus gewollt.

Kein Rocket Science - aber auch kein fauler Kompromiss

Richtlinie BSI TR-03108 fordert unter anderem:

1. Den Einsatz vertrauenswürdiger Zertifikate entsprechend Richtlinie TR-03145
2. Das Vorliegen einer ISO27001-Zertifizierung oder eines IT-Sicherheitskonzeptes nach TKG, sowie die Erfüllung der gesetzlichen Datenschutzvorgaben entsprechend BDSG/GDPR
3. Den Einsatz von DNSSEC
4. Die Sicherung des SSL-Zertifikats durch DANE (TLSA-Records im DNSSEC)
5. Eine aktive Informationspolitik über IT-Sicherheit gegenüber den Usern, u.a. soll offengelegt werden, welche E-Mails mit SSL versendet werden/wurden.

DNSSEC verpflichtend - das erfüllen noch nicht viele

In der Arbeitsgruppe wurden die verschiedenen Anforderungen durchaus kontrovers diskutiert. So wurde lange Zeit DNSSEC nur als wünschenswert erachtet. Erst in der finalen Arbeitsgruppe am 12. April konnte sich unsere Auffassung durchsetzen, dass DNSSEC verpflichtend für sicheren E-Mail-Transport sein muss. Tatsächlich bieten bereits heute sowohl kleinere Anbieter wie mailbox.org als auch große E-Mail-Anbieter wie web.de und GMX dieses Sicherheits-Feature.

Aufwändige, teure Zertifizierung könnte kleine Provider abhalten

Unklar ist aktuell noch, wie die E-Mail-Anbieter an die - aus Marketingsicht erstrebenswerte - Zertifizierung durch das BSI gelangen können. Die entsprechenden Richtlinien liegen aktuell noch nicht in der finalen Fassung vor. Die Arbeitsgruppe kritisiert, dass für die Zertifizierung ein aufwändiger und damit teurer Prüfprozess eines Gutachters vor Ort stattfinden soll. Dagegen argumentieren verschiedene Experten, dass sich 95% der für die Zertifizierung notwendigen Kriterien auch durch automatisierte Tests prüfen lassen.

Entsprechend befürchten vor allem die kleineren E-Mail-Anbieter, dass Aufwand und Kosten kleine und mittelständige Anbieter von der Zertifizierung abhalten, während Großprovider angesichts des zu erwartenden Marketingeffekts die Kosten gerne und problemlos tragen.

Wenn dem BSI an einer flächendeckenden Verbreitung neuer Sicherheitsstandards bei der E-Mail-Kommunikation gelegen ist, muss die Richtlinie nicht nur am technischen Wert, sondern auch daran gemessen werden, ob eine entsprechende Zertifizierung für alle Provider leistbar ist.
(mb)